"Express Mail" Label No.: EV 304937904 US

Date of Deposit: August 22, 2003

Attorney Docket No. 14218US02

A METHOD AND SYSTEM TO PROVIDE PHYSICAL PORT SECURITY IN A DIGITAL COMMUNICATION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS/INCORPORATION BY REFERENCE

[01] This application makes reference to, claims priority to, and claims the benefit of: United States Provisional Application Serial No. 60/462,172 filed April 11, 2003. The above application is incorporated herein by reference in its entirety.

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[02] [Not Applicable]

[SEQUENCE LISTING]

[03] [Not Applicable]

[MICROFICHE/COPYRIGHT REFERENCE]

[04] [Not Applicable]

BACKGROUND OF THE INVENTION

[05] Traditional networking and switching environments rely on destination addresses within frames or packets to determine where the frame or packet is to be forwarded. The destination addresses may be IP (Internet Protocol) addresses or MAC (media access control) addresses, for example.

[06] Security is often provided by maintaining a list of allowed addresses to which frames may be forwarded. A frame of data, having a destination address that is not on the list of allowed addresses, received by a device (e.g., a router) on a digital communication network

can be dropped (i.e., not forwarded). However, users of a communication network can assume identities and apply methods to counter such address-based security techniques.

[07] Further limitations and disadvantages of conventional and traditional approaches will become apparent to one of skill in the art, through comparison of such systems with the present invention as set forth in the remainder of the present application with reference to the drawings.

BRIEF SUMMARY OF THE INVENTION

[08] Aspects of the present invention may be found in a method of providing physical port security including the steps of receiving digital data, inspecting the IP address of the data, generating a destination port bit map of requested physical ports based on the destination information contained in the data, and logically ANDing the generated map with a bit map of the allowed physical destination ports. A further aspect of the method utilizes the source address information in the received data to generate the bit map of allowed physical destinations. An exemplary system of the invention implements physical port security on any intermediate network device, such as a router, for example. The intermediate device contains a bit map of allowed physical destinations that is logically ANDed with the bit map or truth table of requested destinations to create a table of allowed destination ports. Data is only forwarded to ports that are marked as requested AND allowed by the bit map. The bit map of allowed ports may be static or dynamic. For example, the bit map of allowed ports may be generated based on the time of day.

[09] These and other advantages, aspects and novel features of the present invention, as well as details of an illustrated embodiment thereof, will be more fully understood from the following description and drawings.

BRIEF DESCRIPTION OF SEVERAL VIEWS OF THE DRAWINGS

[10] Fig. 1. is a diagram illustrating an embodiment of a digital communication system providing physical port security, in accordance with various aspects of the present invention.

[11] Fig. 2 is a flowchart illustrating an embodiment of a method to provide physical port security in the digital communication system of Fig. 1, in accordance with various aspects of the present invention.

[12] Fig. 3 is a diagram illustrating an embodiment of part of the method of Fig. 2 for performing a logical "AND" operation on two bit maps, in accordance with various aspects of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[13] Certain embodiments of the present invention relate to security on a digital communication network. In particular, certain embodiments of the present invention relate to providing security on a digital communication system at the physical port level.

[14] Fig. 1. is a diagram illustrating an embodiment of a digital communication system 100 providing physical port security, in accordance with various aspects of the present invention. The digital communication system 100 comprises a source device (e.g., a PC) 101, an intermediate network device (e.g., a network router) 102, and nine physical ports, port #1 103 to port #9 111. The source device 101 interfaces to the intermediate network device 102. The intermediate network device 102 interfaces to the physical ports 103-111.

[15] At the physical and datalink layers of a network communication protocol (e.g., the TCP/IP protocol), bits of information are fit into units called data frames. The data frames include source and destination information. Data frames may be classified according to their source and destination ports.

[16] All nodes (clients, servers, routers, etc.) in a network (e.g., a TCP/IP-based network) are assigned an IP address that is written as four numbers between dots, such as 187.5.65.01. The first part of the address is the network address and the second part is the end station address. The network part of the address allows data frames to be routed to a different network. IP addresses are turned into physical station addresses (i.e., MAC addresses) on a network. A data frame is prefixed with an IP header that contains source and destination IP addresses for that data frame.

[17] Network routers contain routing tables that move data frames to the next destination which is either the destination network or another router. In one embodiment, routers inspect only the network part of an address and direct the incoming data frames to the appropriate port for the next "hop" of the routing. Routers move data frames from one hop to the next since a router typically is only aware of devices that are directly connected to the router. A

feature called "multicast" allows a data frame to be delivered to multiple destinations in a digital communication network.

[18] In general, a port in a communication network is a physical point at which signals may enter or leave the network in route to or from another network. Router ports are physical pathways to and from a router connected via a cable.

[19] The nine physical ports 103-111 in Fig. 1 correspond to other devices on the digital communication system 100 which may comprise end stations, other network routers, network bridges, etc. In accordance with an embodiment of the present invention, the source device 101 sends a data frame to the intermediate network device 102. The intermediate network device 102 then sends the data frame to any or all of the physical ports 103-111 based on the destination addresses contained within the data frame and based on the physical port security defined within the intermediate network device 102.

[20] Fig. 2 is a flowchart illustrating an embodiment of a method 200 to provide physical port security in the digital communication system 100 of Fig. 1, in accordance with various aspects of the present invention. In step 201, an intermediate network device receives a data frame from a source device on a communication network. In step 202, the intermediate network device generates a destination port bit map based on destination address information within the received data frame. In step 203, the intermediate network device generates a physical port security bit map based on source address information within the data frame and/or based on port security information within the intermediate network device. In step 204, the intermediate network device performs a logical "AND" operation on the destination port bit map and the physical port security bit map to generate a forwarding port bit map. In step 205, the intermediate network device forwards the data frame to allowed network destinations based on the forwarding port bit map.

[21] Fig. 3 is a diagram illustrating an embodiment of part of the method 200 of Fig. 2 for performing a logical "AND" operation 300 on two bit maps, in accordance with various aspects of the present invention. A physical port security bit map 301 and a destination port

bit map 302 are input to the logical "AND" operation 300. The result is a forwarding port bit map 303 of allowed destinations.

[22] In accordance with an embodiment of the present invention, a bit map essentially comprises a table of "1's" and "0's". A "1" indicates an allowed port and a "0" indicates a disallowed or undesired port. As an example, referring to Fig. 1 and Fig. 3, the physical port security bit map 301 comprises a table of four "1's" and five "0's" corresponding to a total of nine physical ports that the network router 102 is connected to. The four "1's" identify four physical ports (e.g., port #1, port #5, port #6, and port #7) on the network that the network router 102 is allowed to forward frames of data to. The five "0's" identify five physical ports (e.g., port #2, port #3, port #4, port #8, and port #9) on the network that the router is not allowed to forward frames of data to, for security reasons.

[23] In accordance with various embodiments of the present invention, the router 102 may generate a physical port security bit map based on several criteria. For example, the router may keep a pre-defined list of ports it is allowed to communicate with. Also, the router may keep a pre-defined list of source addresses and associated ports, for a given source address, it is allowed to forward data frames to. Therefore, a resultant physical port security bit map may be based on pre-defined security rules for the router and/or pre-defined security rules for a given source. The physical port security bit map may also be defined dynamically. For example, the bit map may be altered or applied based on the time of day, amount of network traffic, or some other variable parameter such as source or destination port utilization or port error rates. Alternatively, the static port security map may be periodically ANDed with the dynamic map to generate the current port security bit map.

[24] When the PC 101 sends a data frame to the network router 102, the network router 102 generates a destination port bit map 302. The destination port bit map 302 is a translation of destination addresses to physical ports. The addresses may be physical MAC addresses of network end stations and bridge ports, or logical ID's. A filtering database within the network router 102 includes addresses associated with each port. The forwarding process of the network router 102 compares the destination address(es) of the received frame to the addresses in the filtering database to generate the destination port bit map 302.

[25] The destination port bit map 302, in the present example, comprises five " 1's " and four " 0's " corresponding to the same nine physical ports (103-111) on the network. The five "1's" identify five physical ports (e.g., port #1, port #3, port #5, port #7, and port #9) that the data frame would like to be forwarded to based on the destination addresses encoded within the data frame.

[26] The logical "AND" operation 300 performed by the network router 102 results in the forwarding port bit map 303 comprising three "1's" and six "0's". As a result, the router 102 will forward the data frame to three of the five port destinations desired by the data frame (i.e., the three port destinations identified by the three "1's" in the forwarding port bit map 303; port #1, port #5, and port #7). Two ports (port #3 and port #9) of the five ports (port #1, port #3, port #5, port #7, and port #9) have been blocked from receiving the data frame for security reasons (i.e., the network router 102 will not forward the data frame to port #3 and port #9 even though the destination addresses in the data frame indicate that the data frame should be forwarded to port #3 and port #9 as well).

[27] In accordance with an alternative embodiment of the present invention, a source device (e.g., PC 101) may perform physical port security for data frames generated within the source device. The source device may generate a physical port security bit map and a destination port security bit map and perform the logical "AND" operation to generate a forwarding port bit map. In general, any device on a digital communication network may perform physical port security, in accordance with various embodiments of the present invention.

[28] In accordance with other alternative embodiments of the present invention, other digital communication system configurations, different from that of Fig. 1, may be implemented as well, also performing physical port security.

[29] In summary, a method and system provide physical port security on a digital communication system. For a given device in the system, security rules may be defined based on associated forwarding ports and/or source devices. Bit mapping techniques and

logical operations may be employed to determine which ports a given data frame from a given source is allowed to be forwarded to.

[30] While the invention has been described with reference to certain embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted without departing from the scope of the invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings of the invention without departing from its scope. Therefore, it is intended that the invention not be limited to the particular embodiment disclosed, but that the invention will include all embodiments falling within the scope of the appended claims.